

LIST OF CLAIMS / AMENDMENTS

In the Claims

Please cancel claims 3, 12, 19-20, 25-31, and 36 without prejudice. Claims 25-31 are canceled as non-elected claims in response to a telephone call from the Examiner on August 25, 2005 for a restriction requirement election (*Office Action* p.2).

Please amend claims 1, 4-8, 11, 16, 23, 32, and 37-41 as shown herein.

Claims 1-2, 4-11, 13-18, 21-24, 32-35, and 37-74 are pending and are listed following:

1. (currently amended) An enterprise network architecture, comprising:
a first network system including one or more first network system domains;
a second network system including one or more second network system domains, the second network system being autonomous from the first network system such that the first network system domains are administratively independent from the second network system domains; and

a trust link between a first network system root domain and a second network system root domain, the trust link configured to provide transitive resource access between the one or more first network system domains and the one or more second network system domains where the transitive resource access includes remote authentication such that an account managed by the second network system can initiate a request for authentication via a first network system domain.

1
2 **2. (original)** An enterprise network architecture as recited in
3 claim 1, wherein:

4 the first network system root domain is configured for communication with
5 the one or more first network system domains;

6 the second network system root domain is configured for communication
7 with the one or more second network system domains; and

8 the trust link is further configured to provide transitive security associations
9 between the one or more first network system domains and the one or more second
10 network system domains.

11
12 **3. (canceled)**

13
14 **4. (currently amended)** An enterprise network architecture as
15 recited in claim 1, wherein the transitive resource access includes the remote
16 authentication to access a resource managed in the second network system, such
17 that ~~an~~ the account managed by the second network system can initiate ~~[[a]]~~ the
18 request for authentication to access the resource via ~~[[a]]~~ the first network system
19 domain.
20
21
22
23
24
25

1 **5. (currently amended)** An enterprise network architecture as
2 recited in claim 1, wherein:

3 [[a]] the first network system domain includes a first domain controller;
4 a second network system domain includes a second domain controller; and
5 ~~an~~ the account managed by the second domain controller can initiate [[a]]
6 the request for remote network authentication via the first domain controller.

7
8 **6. (currently amended)** An enterprise network architecture as
9 recited in claim 1, wherein:

10 [[a]] the first network system domain includes a first domain controller;
11 a second network system domain includes a second domain controller; and
12 ~~an~~ the account managed by the second domain controller can initiate [[a]]
13 the request for authentication to access a resource managed in the second network
14 system, the request for authentication communicated from the first domain
15 controller to the second network system via the trust link.

lee@hayes

4

MS1-680US M01

17 ~~administrator of the first network system, and wherein~~
18 second network system can access resources in the first network system.

19
20 **9. (original)** An enterprise network architecture as recited in
21 claim 1, wherein the trust link is a one-way trust link initiated by an administrator
22 of the first network system, the one-way trust link configured to provide transitive
23 resource access from the second network system domains to the first network
24 system domains.

lee@hayes

5

MS1-680US M01

BEST AVAILABLE COPY

1 **10. (original)** An enterprise network architecture as recited in
2 claim 1, wherein the trust link is a two-way trust link initiated by a first network
3 system administrator and by a second network system administrator, and wherein
4 the transitive resource access is automatically configured when the trust link is
5 established.

6
7 **11. (currently amended)** An enterprise network architecture as
8 recited in claim 1, wherein the first network system is configured to determine
9 from the trust link where to communicate a request for a resource, the request
10 received from ~~an~~ the account managed in the first network system and the resource
11 maintained by the second network system.

12
13 **12. (canceled)**

14
15 **13. (original)** An enterprise network architecture as recited in
16 claim 1, wherein the first network system is configured to receive a request to
17 logon to the second network system and determine from the trust link where to
18 communicate the request, and wherein the second network system is configured to
19 authenticate the request.

20
21 **14. (original)** An enterprise network architecture as recited in
22 claim 1, wherein the trust link is a data structure configured to maintain
23 namespaces corresponding to trusted network system domain components.
24
25

1 **15. (original)** An enterprise network architecture as recited in
2 claim 1, wherein the trust link includes a first network system data structure and a
3 second network system data structure, the first network system data structure
4 configured to maintain trusted namespaces corresponding to the second network
5 system, and the second network system data structure configured to maintain
6 trusted namespaces corresponding to the first network system.

7
8 **16. (currently amended)** An enterprise network architecture as
9 recited in claim 1, wherein the trust link is a data structure configured to maintain
10 namespaces corresponding to the second network system, and wherein the first
11 network system is configured to:

12 maintain the data structure; and
13 automatically designate which of the namespaces are trusted by the first
14 network system.

15
16 **17. (original)** An enterprise network architecture as recited in
17 claim 1, wherein the trust link is a data structure maintained by the first network
18 system, the data structure configured to maintain namespaces corresponding to
19 trusted second network system domain components, and the trusted second
20 network system domain components being designated as trusted by a first network
21 system administrator.

1 **18. (original)** An enterprise network architecture as recited in
2 claim 1, wherein the trust link is a data structure maintained by the first network
3 system, the data structure configured to maintain trusted namespaces
4 corresponding to the second network system, and wherein the first network system
5 is configured to receive a request to logon to the second network system and
6 determine from the trusted namespaces where to communicate the request.

7
8 **19-20. (canceled)**

9
10 **21. (original)** An enterprise network architecture as recited in
11 claim 1, wherein the first network system is configured to:

12 receive an account request to logon to the second network system;

13 determine from the trust link where to communicate the account request;

14 and

15 provide a security identifier to the second network system, the security
16 identifier corresponding to the account.

1 **22. (original)** An enterprise network architecture as recited in
2 claim 1, wherein:

3 the first network system is configured to determine from the trust link
4 where to communicate a service account request to access a resource maintained
5 by the second network system;

6 the first network system is further configured to provide a security
7 identifier to the second network system, the security identifier corresponding to a
8 user account maintained by the first network system; and

9 the second network system is configured to determine from the trust link
10 whether to trust the security identifier to authorize the service account request.

11
12 **23. (currently amended)** An enterprise network architecture as
13 recited in claim 1, wherein the trust link is a data structure maintained by the first
14 network system, the data structure configured to maintain trusted namespaces
15 corresponding to the second network system, and wherein the first network system
16 is configured to:

17 determine from the trusted namespaces where to communicate a logon
18 request received from ~~an~~ the account managed in the second network system; and

19 provide a security identifier to the second network system, the security
20 identifier corresponding to the account.

1 **24. (original)** An enterprise network architecture as recited in
2 claim 1, wherein the trust link is a data structure maintained by the first network
3 system, the data structure configured to maintain trusted namespaces
4 corresponding to the second network system, and wherein:

5 the first network system is configured to determine from the trusted
6 namespaces where to communicate a service account request to access a resource
7 maintained by the second network system;

8 the first network system is further configured to provide a security
9 identifier to the second network system, the security identifier corresponding to a
10 user account maintained by the first network system; and

11 the second network system is configured to determine from the trusted
12 namespaces whether to trust the security identifier to authorize the service account
13 request.

14
15 **25-31. (canceled)**
16
17
18
19
20
21
22
23
24
25

1 **32. (currently amended)** A network system domain, comprising:
2 a root domain controller communicatively linked with one or more network
3 system domains in a first network system; and
4 a trusted domain component configured to define a trust link between the
5 root domain controller and a second network system root domain controller, the
6 second network system root domain controller communicatively linked with one
7 or more second network system domains that are administratively independent
8 from the first network system domains, and the trust link being configured to
9 provide transitive resource access between the first network system domains and
10 the second network system domains, the trusted domain component being further
11 configured to provide remote network authentication such that an account
12 managed by a second network system domain can initiate a request for
13 authentication via a first network system domain.

14
15 **33. (original)** A network system domain as recited in claim 32,
16 wherein the root domain controller is configured to create the trusted domain
17 component when the trust link is initiated.

18
19 **34. (original)** A network system domain as recited in claim 32,
20 wherein the root domain controller is configured to establish the transitive
21 resource access between the first network system domains and the second network
22 system domains when the trust link is initiated.

1 **35. (original)** A network system domain as recited in claim 32,
2 wherein the trusted domain component defines a one-way trust link from the root
3 domain controller to the second network system root domain controller.

4
5 **36. (canceled)**

6
7 **37. (currently amended)** A network system domain as recited in
8 claim 32, wherein the trusted domain component is further configured to provide
9 the remote network authentication to access a resource managed by ~~[[a]]~~ the
10 second network system domain, such that ~~an~~ the account managed by ~~[[a]]~~ the first
11 network system domain can initiate a request to access the resource via ~~the~~
12 ~~network system domain~~, the request communicated from the root domain
13 controller to the second network system root domain controller via the trust link.

14
15 **38. (currently amended)** A network system domain as recited in
16 claim 32, wherein the root domain controller is configured to determine from the
17 trusted domain component where to communicate ~~[[a]]~~ the request for
18 authentication received from ~~an~~ the account managed by ~~[[a]]~~ the second network
19 system domain.

20
21 **39. (currently amended)** A network system domain as recited in
22 claim 32, wherein the trusted domain component is configured to indicate where
23 to communicate ~~[[a]]~~ the request for authentication received from ~~an~~ the account
24 managed by ~~[[a]]~~ the second network system domain.
25

1
2 **40. (currently amended)** A network system domain as recited in
3 claim 32, wherein the root domain controller is configured to determine from the
4 trusted domain component where to communicate a request for a resource, the
5 request received from ~~an~~ the account managed by ~~[[a]]~~ the second network system
6 domain and the resource maintained by the second network system domain.

7
8 **41. (currently amended)** A network system domain as recited in
9 claim 32, wherein the root domain controller is configured to receive a request to
10 logon to ~~[[a]]~~ the second network system domain, and determine from the trusted
11 domain component to communicate the request to the second network system root
12 domain controller via the trust link.

13
14 **42. (original)** A network system domain as recited in claim 32,
15 wherein the trusted domain component is a data structure configured to maintain
16 trusted namespaces corresponding to the second network system.

17
18 **43. (original)** A network system domain as recited in claim 32,
19 wherein the trusted domain component is a data structure configured to maintain
20 namespaces corresponding to trusted second network system domain components.
21
22
23
24
25

1 **44. (original)** A network system domain as recited in claim 32,
2 wherein the trusted domain component is a data structure configured to maintain
3 namespaces corresponding to the second network system, and wherein the root
4 domain controller is configured to maintain the data structure and automatically
5 designate which of the namespaces are trusted by the first network system.

6
7 **45. (original)** A network system domain as recited in claim 32,
8 wherein the trusted domain component is a data structure maintained by the root
9 domain controller, the data structure configured to maintain namespaces
10 corresponding to the second network system, and the namespaces being
11 designated as trusted by a network system administrator.

12
13 **46. (original)** A network system domain as recited in claim 32,
14 wherein the trusted domain component is a data structure maintained by the root
15 domain controller, the data structure configured to maintain trusted namespaces
16 corresponding to the one or more second network system domains, and wherein
17 the root domain controller is configured to receive a request to logon to the second
18 network system and determine from the trusted namespaces where to
19 communicate the request.
20
21
22
23
24
25

1 **47. (original)** A network system domain as recited in claim 32,
2 wherein the trusted domain component is a data structure configured to maintain
3 trusted namespaces corresponding to the second network system, and wherein the
4 root domain controller is configured to determine from the trusted namespaces
5 where to communicate a request for a resource, the request received from an
6 account managed by the root domain controller and the resource maintained by a
7 second network system domain.

8
9 **48. (original)** A network system domain as recited in claim 32,
10 wherein:

11 the trusted domain component is a data structure configured to maintain
12 trusted namespaces corresponding to the second network system;

13 the root domain controller is configured to determine from the trusted
14 namespaces where to communicate a request for a resource, the request received
15 from an account managed by the root domain controller and the resource
16 maintained by a second network system domain; and

17 the second network system is configured to authorize the request for the
18 resource.
19
20
21
22
23
24
25

1 **49. (original)** A network system domain as recited in claim 32,
2 wherein the root domain controller is configured to:

3 receive an account request to logon to a second network system domain;
4 determine from the trusted domain component where to communicate the
5 account request; and

6 provide a security identifier to the second network system domain
7 controller, the security identifier corresponding to the account.

8
9 **50. (original)** A network system domain as recited in claim 32,
10 wherein the trusted domain component is a data structure maintained by the
11 domain controller, the data structure including trusted namespaces corresponding
12 to the second network system, and wherein the root domain controller is
13 configured to:

14 determine from the trusted namespaces where to communicate a logon
15 request received from an account managed by a second network system; and

16 provide a security identifier to the second network system domain
17 controller, the security identifier corresponding to the account.
18
19
20
21
22
23
24
25

1 **51. (original)** A first network system domain controller performing a
2 method comprising:

3 establishing a trust link with a second network system domain controller to
4 provide transitive resource access between domains in a first network system and
5 domains in a separate, autonomous second network system;

6 receiving an authentication request from an account managed by a domain
7 in the second network system; and

8 determining to authenticate the request via the trust link.

9
10 **52. (original)** A method as recited in claim 51, wherein establishing
11 the trust link comprises:

12 receiving network system identifiers corresponding to the second network
13 system;

14 creating a data structure to maintain the network system identifiers; and

15 designating which of the network system identifiers to trust.

16
17 **53. (original)** A method as recited in claim 51, wherein establishing
18 the trust link comprises:

19 receiving namespaces corresponding to the second network system;

20 creating a data structure to maintain the namespaces; and

21 designating which of the namespaces to trust.

1 **54. (original)** A method as recited in claim 51, wherein establishing
2 the trust link comprises:

3 receiving network system identifiers corresponding to the second network
4 system;

5 creating a data structure to maintain the network system identifiers;

6 determining whether to trust an individual network system identifier; and

7 designating in the data structure whether to trust the individual network
8 system identifier.

9
10 **55. (original)** A method as recited in claim 51, wherein establishing
11 the trust link comprises:

12 receiving namespaces corresponding to the second network system;

13 creating a data structure to maintain the namespaces;

14 determining whether to trust an individual namespace; and

15 designating in the data structure whether to trust the individual namespace.

16
17 **56. (original)** A method as recited in claim 51, wherein establishing
18 the trust link comprises:

19 receiving network system identifiers corresponding to the second network
20 system;

21 comparing a received network system identifier with existing network
22 system identifiers to determine whether to accept the received network system
23 identifier; and

24 creating a data structure to maintain accepted network system identifiers.
25

1
2 **57. (original)** A method as recited in claim 51, wherein establishing
3 the trust link comprises:

4 receiving namespaces corresponding to the second network system;
5 comparing a received namespace with existing namespaces to determine
6 whether to accept the received namespace; and
7 creating a data structure to maintain accepted namespaces.

8
9 **58. (original)** A method as recited in claim 51, wherein establishing
10 the trust link comprises receiving network system identifiers corresponding to the
11 second network system and designating which of the network system identifiers to
12 trust, and wherein determining comprises comparing a component of the request
13 with the network system identifiers to determine that the account is managed in
14 the second network system.

15
16 **59. (original)** A method as recited in claim 51, further comprising
17 providing a security identifier corresponding to the account to the first network
18 system domain controller, the first network system domain controller comparing
19 the security identifier with stored network system identifiers to determine whether
20 the security identifier is valid.
21
22
23
24
25

1 **60. (original)** A first network system domain controller performing a
2 method comprising:

3 establishing a trust link with a second network system domain controller to
4 provide transitive resource access between domains in a first network system and
5 domains in a separate, autonomous second network system;

6 receiving a resource request from an account managed by the first network
7 system domain controller;

8 determining to communicate the resource request to the second network
9 system; and

10 communicating the resource request to the second network system domain
11 controller via the trust link.

12
13 **61. (original)** A method as recited in claim 60, wherein establishing
14 the trust link comprises:

15 receiving network system identifiers corresponding to the second network
16 system;

17 creating a data structure to maintain the network system identifiers; and

18 designating which of the network system identifiers to trust.

19
20 **62. (original)** A method as recited in claim 60, wherein establishing
21 the trust link comprises:

22 receiving namespaces corresponding to the second network system;

23 creating a data structure to maintain the namespaces; and

24 designating which of the namespaces to trust.
25

1
2 **63. (original)** A method as recited in claim 60, wherein establishing
3 the trust link comprises receiving network system identifiers corresponding to the
4 second network system and designating which of the network system identifiers to
5 trust, and wherein determining comprises comparing a component of the request
6 with the network system identifiers to determine that the resource is managed in
7 the second network system.

8
9 **64. (original)** A method as recited in claim 60, further comprising
10 providing a security identifier corresponding to the account to the first network
11 system domain controller, the first network system domain controller comparing
12 the security identifier with stored network system identifiers to determine whether
13 the security identifier is valid.
14
15
16
17
18
19
20
21
22
23
24
25

1 **65. (original)** One or more computer-readable media comprising
2 computer-executable instructions that, when executed, direct a first network
3 system domain controller to perform a method comprising:

4 establishing a trust link with a second network system domain controller to
5 provide transitive resource access between domains in a first network system and
6 domains in a separate, autonomous second network system;

7 receiving a resource request from an account managed by a domain
8 controller in the second network system;

9 determining to communicate the resource request to the second network
10 system; and

11 communicating the resource request to the second network system domain
12 controller via the trust link.

13
14 **66. (original)** One or more computer-readable media as recited in
15 claim 65, wherein establishing the trust link comprises:

16 receiving network system identifiers corresponding to the second network
17 system;

18 creating a data structure to maintain the network system identifiers; and

19 designating which of the network system identifiers to trust.
20
21
22
23
24
25

1 **67. (original)** One or more computer-readable media comprising
2 computer-executable instructions that, when executed, direct a domain controller
3 in a first network system to perform a method comprising:

4 requesting network system identifiers corresponding to a second network
5 system to create a trust link between the first network system and the second
6 network system, the second network system being autonomous from the first
7 network system;

8 determining whether to accept the network system identifiers;

9 designating accepted network system identifiers as trusted with trust
10 indicators; and

11 creating a data structure to maintain the accepted network system identifiers
12 and corresponding trust indicators.

13
14 **68. (original)** One or more computer-readable media as recited in
15 claim 67, wherein determining comprises comparing an individual network system
16 identifier with existing network system identifiers and rejecting the individual
17 network system identifier if it is a duplicate of an existing network system
18 identifier.

1 **69. (original)** One or more computer-readable media as recited in
2 claim 67, the method further comprising:

3 receiving an authentication request to logon to a domain in the second
4 network system;

5 comparing a component of the authentication request with the network
6 system identifiers; and

7 communicating the authentication request to the second network system if
8 the component corresponds to a trusted network system identifier.

9
10 **70. (original)** A domain controller in a first network system
11 performing a method, comprising:

12 receiving a security identifier from a domain controller in a second network
13 system via a trust link, the security identifier corresponding to an account
14 managed by the second network system;

15 determining whether the security identifier is valid; and

16 trusting the account corresponding to the security identifier if the security
17 identifier is determined to be valid.

18
19 **71. (original)** A method as recited in claim 70, wherein determining
20 comprises comparing the security identifier with network system identifiers and
21 determining that the security identifier is valid if it matches a component of a
22 network system identifier.

23
24
25

1 **72. (original)** A method as recited in claim 70, wherein determining
2 comprises comparing the security identifier with stored network system identifiers
3 and determining that the security identifier is valid if it matches a component of a
4 network system identifier, the network system identifiers received from the second
5 network system and designated as being trusted when the trust link is initiated.

6
7 **73. (original)** A method as recited in claim 70, wherein the security
8 identifier corresponds to a security principal managed by the domain controller in
9 the second network system.

10
11 **74. (original)** One or more computer-readable media comprising
12 computer-executable instructions that, when executed, direct a computing system
13 to perform the method of claim 70.
14
15
16
17
18
19
20
21
22
23
24
25